



SoftWare Assurance Forum “Common Criteria”

Murray G Donaldson

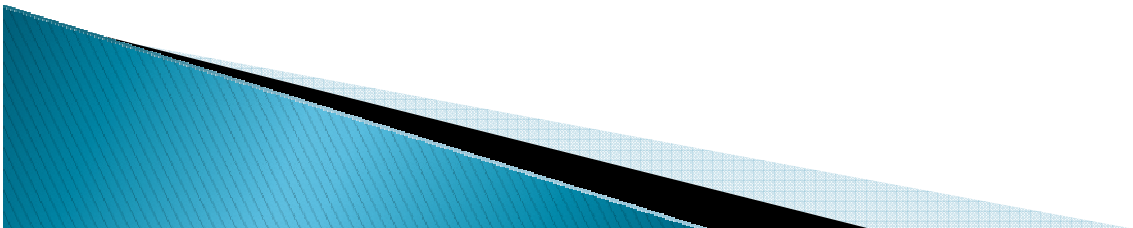
Innovative Intelligent Information Management LLC (I3M LLC)

CC Development Rationale

- ▶ Historically CC based on ‘source’ criteria
 - Focus of ‘source’ criteria was on OS and interps security
 - Backwards compatibility, protection of investment
- ▶ High level aims/objectives statements result
 - CC and CEM that can be considered too general
 - Differing interpretations
 - Insufficient specificity for confidence in recognition
- ▶ CC and CEM needs extension
 - To provide better coverage and clearer applicability to all security products
 - Incorporate latest development in the security environment, e.g. SoftWare Assurance Forum

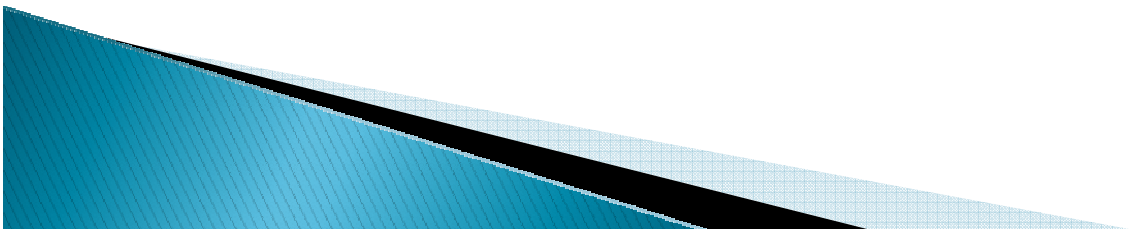
CC Development Process

- ▶ Created Working Groups
 - Evidence Based approaches
 - Skills and Interaction
 - Predictive Assurance
 - Meaningful Reports
 - Tools and Techniques
 - Entry Level Assurance



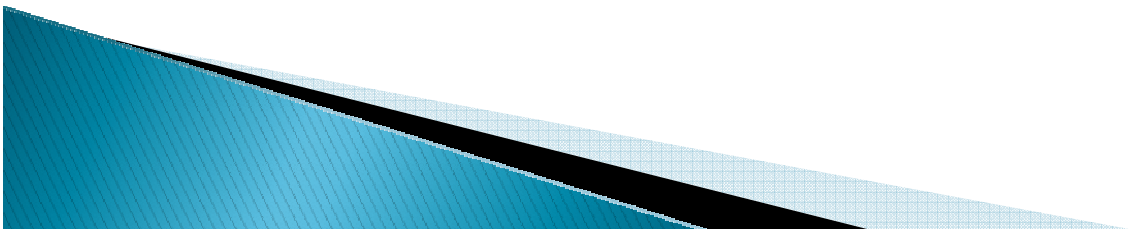
Development Approach

- ▶ Develop range of new 'Standard' PPs
- ▶ Supporting Documents (SDs)
 - Defined technical areas
 - E.g. Smartcards
 - Containing detailed assurance activities
- ▶ Focus development in specific technical areas
 - Engage all stakeholders
- ▶ Engage industry
 - PPs and SDs should be created in concert with industry led consortia



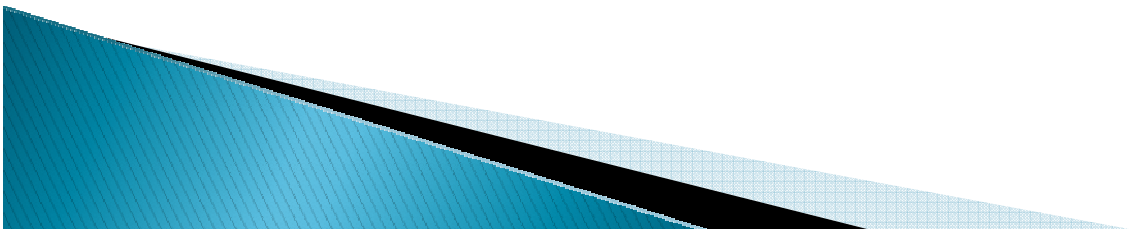
Characteristics of Technical areas

- ▶ Technology used
 - Firewall, database, browser etc.
- ▶ Evaluation approach
- ▶ Evaluation skills
- ▶ Evaluation tools
- ▶ Development approach
- ▶ Threat level addressed
- ▶ Separate grouping of collaborating of vendors, users, evaluators



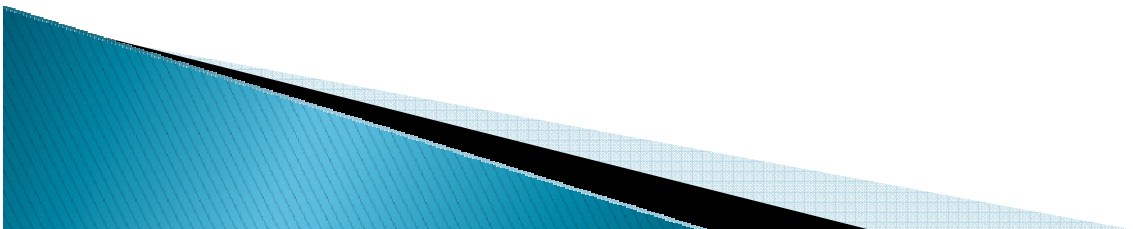
Evidence Based WG

- ▶ Tools and Techniques WG SwA example
 - Propose changes to ADV_* and ALC_TAT
 - Reflect incorporation of software development practices
 - Use of software development tools
 - Results expected to be incorporated in
 - PPs
 - Specification of “refined” assurance requirements
 - SDs
 - Describe secure software assurance development practices and tools
 - Utility & efficacy – the when, where and what etc
 - Integration into the Common Criteria



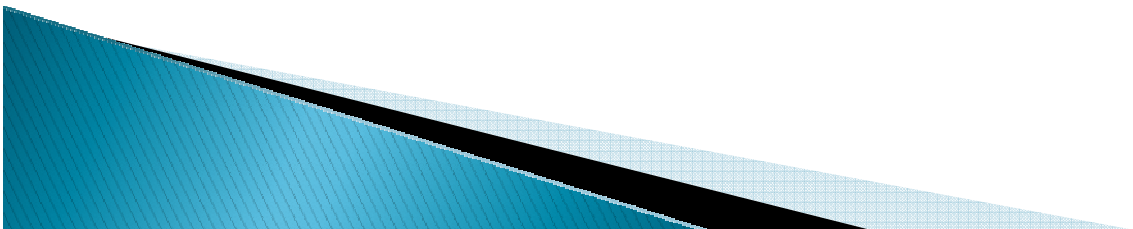
PPs and SDs

- ▶ ALC_TAT proposals taking into account relevant items from the SwA Forum e.g.
 - Common Vulnerabilities and Exposures (CVE)
 - Common Weakness Enumeration (CWE)
 - Common Attack Patterns Enumerations and Configurations (CAPEC)
- ▶ Result will more clearly reflect how to incorporate development practices and the use of software development tools



CC Version 4 Impact?

- ▶ Radical / major changes to the Criteria are neither necessary nor desirable
 - Not necessary – the current criteria are flexible
 - As implemented, can be used for supporting documents
 - Not desirable – radical changes cause overhead
 - Significant change overhead for technology groups e.g. smart card community
- ▶ Some future change for SDs
 - New development practices
 - Wider range of vulnerabilities beyond SwA development



CC Plans

- ▶ CC Development Board (CCDB)
 - Mar/Sep 2010
- ▶ CC Working Groups, Jun/Sep 2010
- ▶ Trials are anticipated
 - Industry partners being sought, by Apr 2010
 - Expected to run thru 2011, report at 12th ICCC
- ▶ Technical Area rationales to be produced by workgroups/consortia
- ▶ CC and CEM updated in annual cycle
 - Without major change
- ▶ 11th ICCC Sep 21–23, 2010 Turkey

